Applicant: Czajkowski et al.
Serial No.: 09/490.941
Group Art Unit: 2132

PATENT

25.   (New) The apparatus of claim 24 wherein said integrated circuit is capable of password protection, thereby requiring a password to access said integrated circuit.

26.   (New) The apparatus of claim 24 wherein said password is user defined.

Remarks

The Applicants submit this amendment in connection with the above-identified application in response to the Office Action mailed March 22, 2001, and the Notice of Non-Compliant Amendment mailed August 24, 2001.

In this Amendment, claims 1-6 have been canceled, claim 7 has been amended, and claim 8-26 have been added. The Applicants note with appreciation the Examiner has indicated claim 7 would be allowable if re-written in accordance with 35 USC §112. Reconsideration of the present application in view of the changes set forth above is hereby requested.

Rejections under 35 USC §112

Claims 3-7 have been rejected under Rejections under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

In response, the Applicants have cancelled claims 1-6, and amended claim 7. By the above amendment it is respectfully submitted that all claims present in the application are in full compliance with 35 USC §112, second paragraph. The Applicants note that such amendments are not intended to limit the claimed invention. Rather, such amendments are being made solely in response to Examiner's rejection under 35 USC §112.

Applicant: Czajkowski et al.
Serial No.: 09/490,941
Group Art Unit: 2132

PATENT

Conclusion

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned **"Version with markings to show changes made."**

Therefore, it is submitted that all pending claims 7-26 are in condition for immediate allowance, and such action is respectfully requested. However, if for any reason direct communication with the Applicant's attorney would serve to advance prosecution of this application to finality, the Examiner is cordially urged to contact the undersigned attorney at the below listed telephone number.

Respectfully submitted,

Dated: _____   _____

                                  Brian Swienton
                                  Reg. No. 49, 030

Brian Swienton, Esq.
Cyberdog Communication, Inc.
689 Lantana St.
La Verne, CA 91750
(909) 394-1897

Applicant: Czajkowski et al.
Serial No.: 09/490.941
Group Art Unit: 2132

PATENT

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In The Claims:

Please cancel claims 1-6, amend claim 7, and add claims 8-26 follows:

7.   (Amended) A method for efficient encryption and decryption of Internet, Intranet, or e-mail messages, comprising the steps of:

providing a sending unit in communication with an integrated encryption circuit embedded with an encryption algorithm;

encrypting a message at [a] said sending unit [which is to be sent to a receiving unit using an integrated circuit embedded with an algorithm located within said sending unit];

appending to the message at said sending unit [the] a receiver's unencrypted IP address;

appending to said message [the] a receiver's encrypted IP address;

[said sending unit sends] sending said encrypted message with said unencrypted IP address and said encrypted IP address to a receiving unit;

providing said receiving unit having an integrated encryption circuit embedded with an decryption algorithm;

[receiving unit with an integrated circuit embedded with an encryption algorithm located within said] receiving with said receiving unit said encrypted message with said unencrypted IP address and said encrypted IP address;

-8-

Applicant: Czajkowski et al.
Serial No.: 09/490,941
Group Art Unit: 2132

PATENT

[receiving unit decrypts] <u>decrypting with said receiving unit</u> said encrypted IP address, <u>thereby resulting in a decrypted IP address;</u> [storing said decrypted IP address in a register built into said integrated circuit embedded encryption algorithm within receiving unit]

<u>storing said decrypted IP address in a first register built into said integrated encryption circuit within receiving unit;</u>

[receiving unit stores] <u>storing</u> said unencrypted IP address into a <u>second</u> register built into said integrated encryption circuit [embedded with an encryption algorithm located] within <u>said</u> receiving unit;

means for comparing said <u>second</u> register storing unencrypted IP address to said <u>first</u> register storing <u>said</u> decrypted IP address;

[receiving unit decrypts] <u>decrypting</u> said message if said <u>second</u> register storing unencrypted IP address matches said <u>first</u> register storing <u>said decrypted</u> [encrypted] IP address; <u>and</u>

means for halting decryption process if said <u>second</u> register storing unencrypted IP address does not match said <u>first</u> register storing <u>said decrypted</u> [encrypted] IP address.

8. <u>(New) A method of encrypting Internet, Intranet, or e-mail messages, comprising:</u>

<u>providing a communication device in communication with a private encryption key generator;</u>

<u>generating a primary private encryption key;</u>

<u>encrypting data with said primary private encryption key;</u>

<u>providing a public encryption key and second private encryption key pair;</u>

<u>encrypting said primary private encryption key and with a public/second private encryption key pair; and</u>

Applicant: Czajkowski et al.
Serial No.: 09/490.941
Group Art Unit: 2132

PATENT

sending said data encrypted with said primary private encryption key and said primary private encryption key encrypted with said public/second private encryption key pair to a receiving unit.

9.   (New) The method of claim 8, wherein access to said private encryption key generator is password controlled.

10.   (New) The method of claim 9 wherein said password is user defined.

11.   (New)The method of claim 8 wherein said encryption key generator is located within a communication device.

12.   (New) The method of claim 8 wherein said primary private encryption key is randomly generated.

13.   (New) A method of decrypting Internet, Intranet, or e-mail messages, comprising:
        providing a communication device in communication with a private encryption key generator;
        receiving an encrypted message with said communication device, said message having data encrypted with a primary private encryption key and a primary private encryption key encrypted with a public/second private encryption key pair;
        providing access to said private encryption key generator;
        decrypting said public/second private encryption key pair with said private encryption key generator, thereby providing said primary private encryption key; and
        decrypting said data with said primary private encryption key.

14.   (New) The method of claim 13 wherein access to said private encryption key generator is password controlled.

Applicant: Czajkowski et al.
Serial No.: 09/490,941
Group Art Unit: 2132

PATENT

15.   (New) The method of claim 14 wherein said password is user defined.

16.   (New) The method of claim 13 wherein access to said primary encryption key generator is requires verification.

17.   (New) The method of claim 16 wherein said verification comprises a Certification of Authority.

18.   (New) A method of encrypting Internet, Intranet, or e-mail messages, comprising the steps of:

       providing a communication device in communication with an integrated encryption circuit embedded with encryption algorithms;

       accessing said integrated encryption circuit to encrypt a message;

       encrypting said with said encryption algorithms;

       providing a message header comprising a sender's private cypher key and a digital bit array;

       encrypting said message header using a receiver's public encryption key;

       appending said encrypted message header to said encrypted message; and

       transmitting said encrypted message header and said encrypted message to a receiver.

19.   (New) The method of claim 18 wherein said message is transmitted through an Internet.

20.   (New) The method of claim 18 wherein said message is transmitted through an Intranet.

21.   (New) The method of claim 18 wherein said message is transmitted through an e-mail.

Applicant: Czajkowski et al.
Serial No.: 09/490,941
Group Art Unit: 2132

PATENT

22. (New) The method of claim 18 wherein said message is transmitted through an wireless communication system.

23. (New) A method decrypting a message of claim 18 further comprising the steps of:

  providing a communication device in communication with a integrated decryption circuit;

  receiving an encrypted message and encrypted message header with said communication device;

  accessing said integrated decryption circuit to decrypt said encrypted message and message header;

  decrypting said message header with said decryption circuit;

  validating said message header with said decryption circuit;

  decrypting said message with said integrated decryption circuit; and

  deleting said private cypher key from said receiver's communication device.

24. (New) An apparatus of encrypting and decrypting Internet, Intranet, and E-mail messages, comprising:

  a communication device;

  an integrated circuit in communication with said communication device;

  a random private cypher key generator embedded within said integrated circuit;

  asymmetric encryption and decryption algorithms embedded within said integrated circuit; and

  symmetric encryption and decryption algorithms embedded within said integrated circuit.

25. (New) The apparatus of claim 24 wherein said integrated circuit is capable of password protection, thereby requiring a password to access said integrated circuit.

26.   (New) The apparatus of claim 24 wherein said password is user defined.